State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

March 16, 2016

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:
SA2016-051

DATE(S) ISSUED:
03/16/2016

SUBJECT:
Multiple Vulnerabilities in Schoolwires Could Allow for Sensitive Information Disclosure

OVERVIEW:
Multiple vulnerabilities have been discovered in Schoolwires, which could result in sensitive information disclosure. Schoolwires is a content management system designed specifically for schools to manage web design and content. These vulnerabilities can be exploited remotely by an attacker with access to a website running Schoolwires. Successful exploitation of these vulnerabilities could allow an attacker to list all files in a user-supplied directory, download arbitrary files, obtain sensitive information of Schoolwires users, or deface the school's website.

It is worth noting that most Schoolwires installations are automatically updated as part of their default configuration settings. The MS-ISAC recommends that this setting be verified to ensure these critical updates are applied.

THREAT INTELLIGENCE:
There is evidence of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:
All Schoolwires versions prior to 2.13 are affected.

RISK:
Government:

- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **Low**
- Small business entities: **Low**

Home users: N/A

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Schoolwires. These vulnerabilities exist due to a failure to sanitize user supplied input in the URL, which could allow exploitation by a non-authenticated remote attacker with access to an affected website.

Successful exploitation of these vulnerabilities could allow an attacker to list all files in a user-supplied directory, download arbitrary files, obtain sensitive information, disclose usernames, email addresses and additional information of Schoolwires users, or deface the school's website.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Verify no unauthorized access or changes have occurred on the system.
- If not utilizing SchoolWires Automatic Updates, apply appropriate patches provided by Schoolwires immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.